UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,680	06/25/2003	Gary L. Graunke	42P16433	3764

8791 7590 02/06/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
02/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/603,680	GRAUNKE ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/20/07 (RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☒ Claim(s) *4,9 and 16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on November 20, 2007 has been entered. Claims 1-30 are pending. At this time, claims 1-30 are still rejected.

Response to Argument

2. Applicant's arguments filed October 29, 2007, with respect to claims 1-30, have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-10 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

a. *Referring to claim 6:*

i. Claim 6 recites "An article of manufacture including a machine readable storage medium encoded with instructions which may be used to program a system to perform a method, comprising: reading an encrypted data block from memory; regenerating, within a predetermined time required to read the encrypted data block from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory; and once reading of the encrypted data block is complete, decrypting the encrypted data block according to the generated keystream.." The claim is directed toward a software

program, and this is a non-statutory subject matter. Furthermore, applicant has pointed out in the specification (see page 16, paragraph 0067 of specification) **"The term "carry" (e.g., a machine readable medium carrying information) thus covers information stored on a storage device or information encoded or modulated into or onto *a carrier wave*."** which clearly including intangible media such as signals, carrier waves, transmissions, optical waves, transmission media or other media incapable of being touched or perceived absent the tangible medium through which they are conveyed. Therefore, claim 6 recites a non-statutory subject matter.

b. *Referring to claims 1-5:*

i. These claims consist a method to implement claim 6, thus they are rejected with the same rationale applied against claim 6 above.

c. *Referring to claims 7-10:*

i. These claims are dependent claims of 6, thus they are rejected with the same rationale applied against claim 6 above.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-2, 5-7, 10, and 21-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doberstein et al (US 5,809148), in view of Monroe et al (US 5,259,025), and further in view of Yup et al (US 6,937,727 B2).

a. *Referring to claim 1:*

i. Doberstein teaches a method comprising:

(1) reading an encrypted data block from memory **(column 3, lines 11-22 of Doberstein);**

(2) regenerating, within a predetermined time required to read the encrypted data block from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory **(see Figure 2 and column 3, lines 11-15 and lines 25-39 of Doberstein);** and

(3) once reading of the encrypted data block is complete, decrypting the encrypted data block according to the generated keystream **(column 3, lines 25-29 of Doberstein).**

ii. Although Doberstein teaches the keystream is either pulled (e.g. read or retrieved) from storage or generated from data stored from the initial receipt of the encrypted data message during the re-transmission of block of encrypted data (column 3, lines 11-22 of Doberstein), Doberstein is not clear in showing whether or not the block of encrypted data is read from storage before the re-transmission process. On the other hand, Monroe clearly teaches this limitation in Figure 4, element 94 and further details on column 1, lines 57-61 of Monroe.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Doberstein (if indeed is not inherent) with the teaching of Monroe for verifying fake-proof video identification data **(column 1, lines 9-10 of Monroe).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Doberstein (if indeed is not inherent) with the teaching of Monroe for validating at a central location a transaction involving presentation of a user identification device at a remote location **(column 1, lines 45-47 of Monroe).**

v. Although the combination of teaching between Dorberstein and Monroe teaches the claimed subject matter, they are silent on the capability of showing the predetermined of number of rounds of a cipher that are reduced to match a memory read latency of the memory. On the other hand, Yup teaches this limitation in column 7, lines 53-67 of Yup.

vi. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the modified-invention of Doberstein with the teaching of Yup for implementing a block cipher algorithm and, more particularly, to a circuit and method for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels. **(column 1, lines 10-15 of Yup).**

vii. The ordinary skilled person would have been motivated to:

(1) have modified the modified-invention of Doberstein with the teaching of Yup for implementing the Advanced Encryption Standard (AES) Rijndaeal block cipher algorithm in a system having a plurality of channels includes one input means in each channel, one cipher key storage means in each channel, key expansion means, encryption/decryption means, and one output means in each channel. **(column 3, lines 18-24 of Yup).**

b. *Referring to claim 2:*

i. Doberstein further teaches:

(1) wherein reading the encrypted data block comprises: receiving a request for the encrypted data block **(column 3, lines 20-22 of Doberstein);** and reading the encrypted data block from a random access memory **(column 3, lines 11-20 of Doberstein).**

c. *Referring to claims 5, 10, 25, 29:*

i. Doberstein further teaches:

(1) wherein decrypting the encrypted data block is performed within a single clock cycle **(column 3, lines 25-29 and column 4, lines 39-41 of Doberstein).**

d. *Referring to claim 6:*

i. This claim consist an article of manufacture including a machine readable medium having stored thereon instructions which may be used to program a system to perform a method claim 1 and thus it is rejected with the same rationale applied against claim 1 above.

e. *Referring to claim 7:*

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

f. *Referring to claims 21-23, 26-28:*

i. These claims consist a processor to implement a method claims 1, and thus it is rejected with the same rationale applied against claim 1 above.

g. *Referring to claim 30:*

i. The combination of teaching between Doberstein, Monroe, and Yup teaches the claimed subject matter. Yup further teaches:

(1) wherein the RAM memory is double data rate (DDR) synchronous data RAM (SDRAM) **(column 2, line 56 of Yup).**

h. *Referring to claim 11:*

i. Doberstein teaches a method comprising:

(1) computing an initialization vector for a data block according to one or more criteria of the data block **(column 8, lines 64-67; column 3, lines 25-39 of Doberstein);** storing the criteria of the data block used to compute the initialization vector for the data block **(column 3, lines 8-10 of Doberstein);** computing a keystream from the initialization vector and a secret key using a predetermined number of round of a cipher that are reduced to match a memory read latency of a memory **(column 3, lines 11-39 of Doberstein);** encrypting the data block according to

the keystream **(column 1, lines 53-65 of Doberstein);** and storing the encrypted data block within memory **(column 3, lines 8-10 of Doberstein).**

ii. Although Doberstein teaches the keystream is either pulled (e.g. read or retrieved) from storage or generated from data stored from the initial receipt of the encrypted data message during the re-transmission of block of encrypted data (column 3, lines 11-22 of Doberstein), Doberstein is not clear in showing whether or not the block of encrypted data is read from storage before the re-transmission process. On the other hand, Monroe clearly teaches this limitation in Figure 4, element 94 and further details on column 1, lines 57-61 of Monroe.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Doberstein (if indeed is not inherent) with the teaching of Monroe for verifying fake-proof video identification data **(column 1, lines 9-10 of Monroe).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Doberstein (if indeed is not inherent) with the teaching of Monroe for validating at a central location a transaction involving presentation of a user identification device at a remote location **(column 1, lines 45-47 of Monroe).**

v. Although the combination of teaching between Dorberstein and Monroe teaches the claimed subject matter, they are silent on the capability of showing the predetermined of number of rounds of a cipher that are reduced to match a memory read latency of the memory. On the other hand, Yup teaches this limitation in column 7, lines 53-67 of Yup.

vi. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the modified-invention of Doberstein with the teaching of Yup for implementing a block cipher algorithm and, more particularly, to a circuit and method for implementing the Advanced Encryption Standard (AES) block cipher algorithm in a system having a plurality of channels. **(column 1, lines 10-15 of Yup).**

vii. The ordinary skilled person would have been motivated to:

(1) have modified the modified-invention of Doberstein with the teaching of Yup for implementing the Advanced Encryption Standard (AES) Rijndaeal block cipher algorithm in a system having a plurality of channels includes one input means in each channel, one cipher key storage means in each channel, key expansion means, encryption/decryption means, and one output means in each channel. **(column 3, lines 18-24 of Yup)**

i. *Referring to claim 12:*

i. Doberstein further teaches:

(1) wherein computing the initialization vector comprises: receiving a write request for the data block **(column 3, lines 11-12 of Doberstein);** identifying a page containing the data block **(column 3, lines 60-65 of Doberstein);** forming a page initialization vector according to the page containing the data block as the initialization vector of the data block **(column 3, lines 25-39 of Doberstein).**

j. *Referring to claims 13-14:*

i. These claims have limitations that is similar to those of claim 12, thus they are rejected with the same rationale applied against claim 12 above.

k. *Referring to claim 15:*

i. Doberstein further teaches:

(1) wherein forming the block initialization vector comprises: selecting a block counter value for page writes to the page containing the data block as the block initialization vector **(column 3, lines 55-65 of Doberstein)**.

l. *Referring to claim 17:*

i. Doberstein further teaches:

(1) wherein computing the keystream comprises: providing the initialization vector and the secret key to one of a stream cipher and a block cipher to generate the keystream **(column 3, lines 25-39 of Doberstein)**.

f. *Referring to claims 18-20:*

i. These claims have limitations that are similar to those of claims 11-15, thus they are rejected with the same rationale applied against claims 11-15 above.

g. *Referring to claim 24:*

i. The combination of teaching between Doberstein, Monroe, and Yup teaches the claimed subject matter. Monroe further teaches:

(1) wherein the decrypt logic decrypts encrypted data block within a single clock cycle using an exclusive-OR operation (column 7, lines 1-4)

7. Claims 3, 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doberstein et al (US 5,809148), in view of Monroe et al (US 5,259,025), in view of Yup et al (US 6,937,727 B2)., and further in view of Lynn et al (US 5,345,508).

a. *Referring to claims 3, 8:*

i. Athough Doberstein's modified invention teaches the claimed subject matter using in an initialization vector in the encryption process, they are silent on the capability of using an initial portion of initialization vector in the encryption process.

(1) wherein re-generating the keystream comprises: identifying an initial portion of an initialization vector used to encrypt the data block according to a page containing the encrypted data block; identifying a remaining portion of the initialization vector used to encrypt the data block according to a block number of the data block; and recomputing the keystream according to the identified initial portion of initialization vector and the identified remaining portion of the initialization vector and a secret key **(column 3, lines 30-39 of Doberstein).**

ii. On the other hand, Lynn teaches the portion of initialization vector in column 3, lines 38-39 of Lynn.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the modified-invention of Doberstein with the teaching of Lynn for processing initialization vectors or initial values **(column 2, lines 60-65 of Lynn).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the modified-invention of Doberstein with the teaching of Lynn to implementing a cryptography engine.

Allowable Subject Matter

8. Claims 4, 9, 16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT

February 2, 2008

THANHNGA TRUONG
PRIMARY EXAMINER